Vermont . . .

Department of Banking, Insurance, Securities and Health Care Administration

---

STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

REGULATION IH-2002-03

Table of Contents

Section 1. Preamble & Authority

A. This regulation establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, consistent with sections 501, 505(b), and 507 of the Gramm-Leach-Bliley Act, codified at 15 U.S.C. 6801, 6805(b) and 6807 and 8 V.S.A. § § 15, 3568, 3688, 4812, 5111, and 8014.

B. Section 501(a) of the Gramm-Leach-Bliley Act provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) and 505 (b) (2) require the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer.

C. Section 505(b)(2) calls on state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by regulation with respect to persons engaged in providing insurance.

D. Section 507 provides, among other things, that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This regulation requires that the safeguards established pursuant to this regulation shall apply to nonpublic personal information, including nonpublic personal financial information and nonpublic personal health information.

Section 2. Definitions

For purposes of this regulation, the following definitions apply:

A. "Customer" means a customer of the licensee as the term customer is defined in Section 4.I of Regulation IH-2001-01, Privacy of Consumer Financial and Health Information Regulation.

B. "Customer information" means nonpublic personal information as defined in Section 4.S of Regulation IH-2001-01, Privacy of Consumer Financial and Health Information about a customer, whether in paper, electronic or other form, that is maintained by or on behalf of the licensee.

C. "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect or dispose of customer information.

D. "Licensee" means a licensee as that term is defined in Section 4.Q of Regulation IH-2001-01, Privacy of Consumer Financial and Health Information, except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the surplus lines business conducted pursuant to chapter 138 of title 8 V.S.A.

E. "Service provider" means a person that maintains, processes or otherwise is permitted access to customer information through its provision of services directly to the licensee.

Section 3. Information Security Program

Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

Section 4. Objectives of Information Security Program

A licensee's information security program shall be designed to:

A. Ensure the security and confidentiality of customer information;

B. Protect against any anticipated threats or hazards to the security or integrity of the information; and

C. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Section 5. Examples of Methods of Development and Implementation

The actions and procedures described in Sections 6 through 9 of this regulation are examples of methods of implementation of the requirements of Sections 3 and 4 of this regulation. These examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Sections 3 and 4 of this regulation.

Section 6. Risk Assessment

The licensee:

A. Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

B. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

C. Assesses the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.

Section 7. Management and Control of Risk

The licensee:

A. Designs its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities;

B. Trains staff, as appropriate, to implement the licensee's information security program; and

C. Regularly tests or otherwise regularly monitors the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.

Section 8. Oversight of Service Provider Arrangements

The licensee:

A. Exercises appropriate due diligence in selecting its service providers; and

B. Requires its service providers to implement appropriate measures designed to meet the objectives of this regulation, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied these obligations.

Section 9. Program Adjustment

The licensee monitors, evaluates and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.

Section 10. Violations

In addition to any other sanctions available to the commissioner under Vermont law for violations of this regulation, any violation of this rule shall be subject to the powers and penalties set forth in 8 V.S.A. 3661.

Section 11. Severability

If any section or portion of a section of this regulation or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation or the applicability of the provision to other persons or circumstances shall not be affected.

Section 12. Effective Date

This regulation is effective 30 days from the date of adoption. Each licensee shall establish and implement an information security program, including appropriate policies and systems pursuant to this regulation by October 10, 2003.

John P. Crowley, Commissioner